532,193

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
21 mai 2004 (21.05.2004)

PCT

(10) Numéro de publication internationale
WO 2004/043036 A1

(51) Classification internationale des brevets[7] :
H04L 29/06, 9/08

(21) Numéro de la demande internationale :
PCT/FR2003/003250

(22) Date de dépôt international :
30 octobre 2003 (30.10.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0213982 30 octobre 2002 (30.10.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : THOMSON LICENSING S.A. [FR/FR]; 46 Quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : DURAND, Alain [FR/FR]; 79, rue de Dinan, F-35000 Rennes (FR). ANDREAUX, Jean-Pierre [FR/FR]; 20 rue de Lorgeril, F-35000 Rennes (FR).

(74) Mandataire : BERTHIER, Karine; Thomson, 46 Quai Alphonse Le Gallo, F-92648 Boulogne cedex (FR).

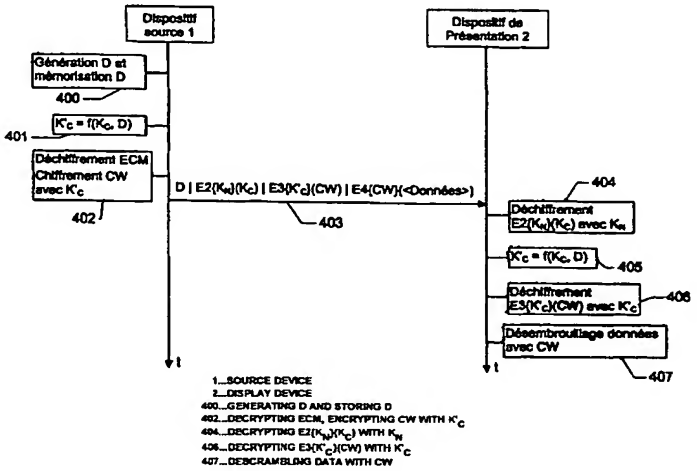
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

[Suite sur la page suivante]

(54) Title: SIMPLIFIED METHOD FOR RENEWING SYMMETRICAL KEYS IN A DIGITAL NETWORK

(54) Titre : PROCEDE SIMPLIFIE DE RENOUVELLEMENT DE CLES SYMETRIQUES DANS UN RESEAU NUMERIQUE



(57) Abstract: The invention concerns a method implemented in a communication network comprising a source device (1) including: a first symmetrical key (K_C) for encrypting data (CW) to be transmitted to a display device (2) connected to the network; and the first symmetrical key (K_C) encrypted ($E2\{K_N\}(K_C)$) with a second symmetrical network key (K_N) known only to at least one display device (2) connected to the network. When the source device needs to renew its first symmetrical key (K_C) to encrypt new data, it generates a random number (D), then it calculates a new symmetrical key (K'_C) based on the first symmetrical key (K_C) and on the random number (D). It then encrypts the data to be transmitted (CW) with the new symmetrical key (K'_C) and transmits to a display device, via the network: the data encrypted with the new symmetrical key ($E3\{K'_C\}(CW)$), the random number (D), and the first encrypted symmetrical key with the second symmetrical network key ($E3\{K'_C\}(CW)$).

[Suite sur la page suivante]

WO 2004/043036 A1

européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Le procédé de l'invention est mis en uvre dans un réseau de communication comprenant un dispositif source (1)qui contient :- une première clé symétrique (KC) pour chiffrer des données (CW) ô transmettre ô un dispositif de présentation (2) raccordé au réseau ; et - la première clé symétrique (KC) chiffrée (E2{KN}(KC)) avec une seconde clé symétrique de réseau (KN) connue seulement d'au moins un dispositif de présentation (2) raccordé au réseau. Lorsque le dispositif source doit renouveler sa première clé symétrique (KC) pour chiffrer de nouvelles données, il génère un nombre aléatoire (D), puis il calcule une nouvelle clé symétrique (K'C) en fonction de la première clé symétrique (KC) et du nombre aléatoire (D). Il chiffre ensuite les données ô transmettre (CW) avec lanouvelle clé symétrique (K'C) puis il transmet ô un dispositif de présentation, via le réseau : - les données chiffrées avec la nouvelle clé symétrique (E3{K'C}(CW)) ; - le nombre aléatoire (D) ; et - la première clé symétrique chiffrée avec la seconde clé symétrique de réseau (E2{KN}(KC)).

Procédé simplifié de renouvellement de clés symétriques dans un réseau numérique

Domaine de l'invention

La présente invention se rapporte d'une manière générale au domaine de la gestion de clés cryptographiques dans des réseaux numériques locaux et plus particulièrement dans des réseaux numériques domestiques.

Etat de la technique

Un tel réseau est constitué d'un ensemble de dispositifs reliés entre eux par un bus numérique, par exemple un bus selon la norme IEEE 1394. Il comprend notamment deux types de dispositifs :

- Des dispositifs sources capables d'émettre des données sur le réseau : Ces dispositifs peuvent récupérer les données à travers un « canal » externe au réseau.

- Des dispositifs de présentation, adaptés à recevoir les données circulant sur le réseau, pour les traiter ou les présenter à l'utilisateur.

Ainsi, si on prend l'exemple d'un réseau numérique domestique destiné à véhiculer des données audio et/ou vidéo dans différentes pièces d'une maison, les dispositifs sources sont par exemple des décodeurs numériques recevant des programmes vidéo de l'extérieur du réseau, via une antenne satellite ou via une connexion au câble, ou bien des lecteurs de disques optiques diffusant sur le réseau, sous forme numérique, des données (audio et/ou vidéo) lues sur un disque (le disque contient dans ce cas des données provenant de l'extérieur du réseau). Les dispositifs de présentation sont par exemple des récepteurs de télévision permettant de visualiser des programmes vidéo reçus du réseau ou, d'une manière plus générale tout type d'appareil ayant la capacité de déchiffrer des données chiffrées.

Si on se place du point de vue des fournisseurs de contenu qui fournissent les données en provenance de l'extérieur du réseau local, notamment des prestataires de services diffusant des programmes télévisés payants ou bien des éditeurs de disques optiques par exemple, il est nécessaire d'éviter que ces données transmises ne soient copiées et puissent circuler facilement (par exemple en étant copiées sur un disque optique ou tout autre support d'enregistrement) d'un réseau local à l'autre.

Pour cela, il est connu de transmettre les données sous forme secrète en les chiffrant à l'aide d'algorithmes de cryptographie utilisant des clés qui sont connues au préalable des appareils autorisés à recevoir ces données ou bien qui sont échangées selon des protocoles particuliers sécurisés entre le fournisseur de contenu et ces appareils.

La demande de brevet PCT WO 00/62505 au nom de THOMSON multimédia, déposée le 31 mars 2000 et revendiquant la priorité d'une demande de brevet française au nom du même demandeur, déposée le 13 avril 1999 et publiée sous la référence FR 2792482, concerne un réseau domestique dans lequel une clé publique propre au réseau est utilisée pour chiffrer les données circulant entre des appareils du réseau, typiquement des dispositifs sources précédemment mentionnés vers des dispositifs de présentation. Seuls les appareils de présentation de ce réseau possèdent la clé privée correspondant à la clé publique. Le couple (clé publique, clé privée) étant spécifique au réseau, des données chiffrées dans le cadre de ce réseau ne peuvent être déchiffrées par des appareils d'un autre réseau.

L'utilisation d'un couple de clés asymétriques présente certains avantages, mais aussi quelques inconvénients. Un des principaux avantages est qu'aucun secret n'est mémorisé dans les appareils sources: ces appareils ont connaissance de la clé publique, mais non de la clé privée. Cependant, la mise en œuvre de clés asymétriques est d'une relative lenteur, par rapport à celle de clés symétriques. De plus, la durée de vie de clés asymétriques est faible, exigeant une révocation périodique et la création de nouvelles clés. Dans ce cas, des données chiffrées avec une clé, puis enregistrées, pourraient soudainement ne plus être déchiffrables sur le réseau. De plus, un nombre important de paires de clés asymétriques est nécessaire.

On serait alors tenté par la mise en oeuvre d'une clé symétrique pour chiffrer les données. Or, cela exigerait que les dispositifs source aient connaissance de cette clé, ce qui leur imposerait des contraintes de sécurité accrues et les rendrait par conséquent plus onéreux.

La présente invention vise à résoudre les problèmes précités.

Exposé de l'invention

L'invention a pour objet un procédé de renouvellement de clé symétrique dans un réseau de communication comprenant un dispositif d'un premier type contenant :

- une première clé symétrique pour chiffrer des données à transmettre à un dispositif d'un second type raccordé au réseau ; et
- ladite première clé symétrique chiffrée avec une seconde clé symétrique de réseau connue seulement d'au moins un dispositif d'un second type raccordé audit réseau.

Selon le procédé, le dispositif d'un premier type génère un nombre aléatoire, puis il calcule une nouvelle clé symétrique en fonction de la première clé symétrique et du nombre aléatoire. Il chiffre ensuite les données à transmettre avec la nouvelle clé symétrique puis il transmet à un dispositif d'un second type, via le réseau :

- les données chiffrées avec la nouvelle clé symétrique;
- le nombre aléatoire; et
- la première clé symétrique chiffrée avec la seconde clé symétrique de réseau.

Le procédé peut en outre comporter les étapes qui consistent, pour le dispositif d'un second type qui reçoit les données transmises par le dispositif d'un premier type, à déchiffrer, avec la seconde clé symétrique de réseau, le chiffrement de la première clé symétrique ; puis à déterminer, en fonction de la première clé symétrique ainsi obtenue et du nombre aléatoire reçu, la nouvelle clé symétrique ; et à déchiffrer les données reçues avec la nouvelle clé symétrique ainsi obtenue.

Brève description des dessins

D'autres caractéristiques et les avantages de l'invention apparaîtront à travers la description d'exemples de réalisation particuliers non limitatifs, explicité à l'aide des figures jointes, parmi lesquelles :

- la figure 1 est un schéma bloc d'un réseau de communication reliant plusieurs appareils dans lequel est mise en œuvre l'invention;
- les figures 2 et 3 sont des diagrammes temporels illustrant les communications entre un dispositif source de données chiffrées et un dispositif de présentation desdites données dans un tel réseau selon un mode de réalisation de l'invention.

Description détaillée de modes de réalisation de l'invention

On décrira dans un premier temps un exemple de réseau de communication pour illustrer la façon dont les données et les clés diverses sont

échangées. Par la suite, on décrira de manière plus détaillée la gestion proprement dite des clés et leur utilisation pour une transmission de données sécurisée entre un dispositif source et un dispositif de présentation.

I] Description du réseau

Sur la figure 1, on a représenté un réseau numérique domestique comprenant un dispositif source 1, un dispositif de présentation 2 et un dispositif d'enregistrement 3 reliés ensembles par un bus numérique 4, qui est par exemple un bus selon la norme IEEE 1394.

Le dispositif source 1 comprend un décodeur numérique 10 doté d'un lecteur de carte à puce muni d'une carte à puce 11. Ce décodeur reçoit des données numériques, notamment des programmes audio/vidéo distribués par un prestataire de service.

Le dispositif de présentation 2 comprend un récepteur de télévision numérique (DTV) 20 doté d'un lecteur de carte à puce muni d'une carte à puce 21 et le dispositif d'enregistrement 3 est notamment un magnétoscope numérique (DVCR).

Les données numériques qui entrent sur le réseau via le dispositif source 1 sont en général des données embrouillées par un fournisseur de contenu, par exemple selon le principe de la télévision payante. Dans ce cas, les données sont embrouillées à l'aide de mots de contrôle CW (de l'anglais « Control Word ») qui sont eux-mêmes transmis dans le flux de données sous forme chiffrée à l'aide d'une clé de chiffrement K_F en étant contenus dans des messages de contrôle ECM (de l'anglais « Entitlement Control Message »). La clé de chiffrement K_F est mise à la disposition des utilisateurs qui ont payé pour recevoir les données, notamment en étant stockée dans une carte à puce. Dans l'exemple de la figure 1, la carte à puce 11 contient une telle clé K_F ainsi qu'un module d'accès conditionnel CA 14 capable de déchiffrer les mots de contrôle CW.

On notera cependant que bien souvent, l'autorisation de recevoir les données n'est que temporaire, tant que l'utilisateur paie un abonnement au fournisseur de contenu. La clé K_F est donc modifiée régulièrement par le fournisseur de contenu. Grâce au procédé qui sera décrit ci-dessous, l'utilisateur pourra néanmoins enregistrer des programmes transmis pendant qu'il est abonné et les relire autant de fois qu'il le souhaite sur son propre réseau, même lorsque la clé K_F aura été changée. Par contre, comme les

données sont enregistrées sous forme embrouillée de la manière décrite, elles ne pourront être relues que sur le réseau de l'utilisateur qui les a enregistrées.

Le dispositif source 1 qui reçoit ces données numériques embrouillées les met ensuite en forme pour qu'elles soient diffusées sur le réseau numérique selon un format de protection spécifique au réseau domestique. Le décodeur 10 comporte un module « unité ECM » 13 qui extrait du flux de données reçu les messages ECM contenant les mots de contrôle chiffrés à l'aide de la clé K_F pour les transmettre au module CA 14. Celui-ci déchiffre les mots de contrôle CW et les transmet à un module convertisseur 12 également contenu dans la carte à puce 11.

Le module convertisseur 12 contient une clé symétrique K_C dont la génération et la transmission entre les appareils du réseau seront décrites ultérieurement.

On notera que sur la figure 1, le réseau est représenté dans l'état dans lequel il se trouve lorsque tous les appareils ont été raccordés et ont échangé des clés cryptographiques selon des procédés qui seront décrits ultérieurement. La figure 1 illustre en particulier, pour le dispositif source 1 et le dispositif de présentation 2, toutes les clés contenues dans chaque dispositif. Les clés représentées ne sont pas forcément présentes à tout moment dans les dispositifs.

En particulier, le dispositif de présentation 2 comporte dans une mémoire une clé symétrique de réseau K_N. Cette clé est distribuée à tout nouveau dispositif de présentation nouvellement connecté au réseau selon un procédé sécurisé qui ne fait pas l'objet de la présente invention et ne sera pas décrit davantage. De plus, chaque dispositif de présentation possède une paire de clés asymétriques (K_{PUBT}, K_{PRIT}), la première clé étant publique et la seconde privée. Ces clés sont utilisées dans le cadre de l'authentification des appareils du réseau, ainsi que pour l'échange initial des clés symétriques comme on le verra ultérieurement.

Le module convertisseur 12 utilise la clé symétrique K_C pour chiffrer les mots de contrôle CW et il insère ces mots de contrôle chiffrés dans des messages notés LECM (de l'anglais « Local Entitlement Control Message »). Ces messages LECM ont la même fonction que les messages ECM inclus dans le flux de données reçus initialement, à savoir transmettre les mots de contrôle sous une forme protégée, mais dans les messages LECM, les mots de contrôle CW y sont chiffrés à l'aide de la clé symétrique K_C au lieu d'être chiffrés à l'aide de la clé K_F du fournisseur de contenu.

De préférence, la clé K_C est fréquemment renouvelée, par exemple lors de l'initiation de chaque transmission de données, dans le but d'éviter que le dispositif source ne comporte un secret à long terme, qui exigerait une protection renforcée.

Le module convertisseur 12 insère en outre dans les messages LECM la clé symétrique K_C elle même, mais chiffrée à l'aide d'une autre clé symétrique K_N par un algorithme E2, c'est à dire $E2\{K_N\}(K_C)$.

Dans le reste de la description, on utilisera toujours la notation « E{K}(M) » pour signifier chiffrement de données M par un algorithme E avec une clé K.

La clé K_N, que nous appellerons dans la suite clé de réseau, ne réside pas dans l'appareil source 1, mais dans l'appareil de présentation 2. Suite à la création de la clé K_C, cette dernière est transmise de manière sécurisée à l'appareil de présentation 2, qui la chiffre à l'aide de K_N et retransmet le résultat à l'appareil source qui le mémorise dans le module convertisseur 12 de sa carte, pour utilisation ultérieure.

Les messages LECM ainsi construits sont ensuite transmis à l'unité ECM 13 qui les insère dans le flux de données à la place des messages ECM. Il est à noter que lorsque le contenu reçu n'est pas déjà sous forme embrouillée comme décrit ci-dessus et ne contient pas de message ECM, le module convertisseur 12 est chargé dans ce cas de mettre les données sous cette forme pour que le flux de données diffusé sur le bus 4 soit toujours sous la forme de paquets de données tels le paquet 40 représenté à la figure 1 contenant un message LECM et des données embrouillées.

On peut résumer le contenu de ce paquet comme suit :

LECM | E4{CW}(<données>) ; soit :

$E2\{K_N\}(K_C)$ | $E3\{K_C\}(CW)$ | E4{CW}(<données>) ;

où « | » représente l'opérateur de concaténation.

Les données circulent donc toujours sous forme chiffrée dans le bus 4, et seuls les appareils ayant accès à la clé symétrique K_C sont capables de déchiffrer les mots de contrôles CW et donc de déchiffrer les données. Ces appareils sont ceux possédant la clé de réseau K_N. Ceci empêche donc la diffusion vers d'autres réseaux locaux de toute copie effectuée dans le réseau domestique de la figure 1.

Lorsque les paquets de données 40 sont reçus par le récepteur de télévision numérique 20, ils sont transmis au module « Unité LECM » 23 qui en extrait les messages LECM pour les transmettre à un module terminal 22

contenu dans la carte à puce 21. Ce dernier déchiffre tout d'abord $E2\{K_N\}(K_C)$ à l'aide de la clé K_N qu'il contient pour obtenir la clé K_C. Ensuite, à l'aide de la clé K_C, il déchiffre $E3\{K_C\}(CW)$ pour obtenir le mot de contrôle CW qu'il transmet au module « Unité LECM » 23. Celui-ci est alors en mesure de désembrouiller les données E4{CW}(<données>) à l'aide du mot de contrôle. Les données désembrouillées sont ensuite présentées à l'utilisateur. Dans le cas de données vidéo, celles-ci peuvent être visualisées sur le récepteur de télévision 20.

Grâce au réseau numérique local qui vient d'être décrit, le flux de données numériques reçu d'un fournisseur de contenu est transformé par le dispositif source qui le reçoit en un flux de données dans lequel les données (ou plus précisément les mots de contrôle CW) sont chiffrées avec à une clé symétrique K_C. La clé K_C est transmise avec les données chiffrées avec son aide, en étant elle-même chiffrée à l'aide d'une autre clé symétrique, la clé de réseau K_N. Le flux de données qui circule dans le réseau local contient ainsi des données ayant un format spécifique à ce réseau local qui ne peuvent être déchiffrées que par les dispositifs de présentation du réseau local qui contiennent tous la clé du réseau K_N.

De plus, comme la clé K_C est diffusée avec les données (sous forme chiffrée), elle peut être enregistrée, par exemple par le magnétoscope numérique (DVCR) 4, en même temps que les données ce qui permettra un accès ultérieur aux données chiffrées.

Par ailleurs, comme la clé de réseau K_N n'est pas stockée dans les dispositifs sources, ceux-ci ne contiennent donc pas de secret « long terme », exigeant des précautions de sécurité accrues.

La clé K_C doit cependant être renouvelée fréquemment et nous allons maintenant décrire plus précisément comment cette clé K_C est générée et comment son chiffrement à l'aide de la clé de réseau K_N est obtenu selon différentes variantes.

II] Génération et gestion de la clé symétrique K_C lors d'une première connexion au réseau d'un dispositif source

Supposons que le dispositif source 1 vient juste d'être connecté au réseau domestique illustré à la figure 1. Il ne possède au départ aucune clé dans son module convertisseur 12.

Le figure 2 illustre les étapes d'un protocole initial permettant au dispositif source d'obtenir une clé symétrique K_C chiffrée à l'aide de la clé de réseau K_N détenue par un dispositif de présentation du réseau.

Lors d'une première étape 101, le dispositif source 1 lance une requête sur le réseau, demandant à tout dispositif de présentation de lui transmettre sa clé publique. Sur la figure 1, nous avons représenté un seul dispositif de présentation mais naturellement, le réseau numérique domestique peut comporter plusieurs dispositifs de présentation différents raccordés au bus 4. Tous les dispositifs de présentation présents et en état « d'éveil » sur le réseau (c'est à dire ceux dont l'alimentation n'est pas coupée ou bien qui ne sont pas dans un mode de mise en veille avec une alimentation très réduite des circuits du dispositif) sont supposés répondre à la requête du dispositif source en renvoyant leur clé publique

Nous supposerons dans la suite que la première clé reçue par le dispositif source 1 est la clé publique K_{PUBT} envoyée au cours de l'étape 102 par le dispositif de présentation 2. Le dispositif source 1 prend en compte le premier message reçu et échangera ensuite des messages avec le dispositif de présentation correspondant.

Le dispositif source 1, et plus précisément le module convertisseur 12, génère ensuite de manière aléatoire une clé symétrique « court terme » K_C et il mémorise cette clé K_C (étape 103). Il utilise par exemple pour la génération de K_C un générateur de nombre pseudo-aléatoire.

La clé K_C est ensuite chiffrée à l'étape 104 avec la clé publique K_{PUBT} par l'intermédiaire d'un algorithme de chiffrement asymétrique E1, par exemple l'algorithme « RSA OAEP » (pour « Rivest, Shamir, Adleman Optimal Asymmetric Encryption Padding » – décrit dans « *PKCS#1: RSA Cryptography Specifications, version 2.0 (October 1998)* »), puis transmise sous forme chiffrée $E1\{K_{PUBT}\}(K_C)$ au dispositif de présentation 2 (étape 105). Ce dernier déchiffre la clé K_C à l'aide de sa clé privée KPRIT puis il la chiffre de nouveau selon un algorithme de chiffrement symétrique E2 à l'aide de la clé symétrique de réseau K_N (étape 106) et renvoie K_C ainsi chiffrée (i.e. $E2\{K_N\}(K_C)$) au dispositif source (étape 107), qui mémorise cette information (étape 108), de préférence dans son module convertisseur 12.

A l'issu de cette première série d'étapes 101 à 108, le dispositif source 1 possède donc dans son module convertisseur 12, une clé symétrique K_C qui va pouvoir être utilisée pour chiffrer des données, typiquement des mots de contrôles CW, et le chiffrement de cette clé K_C à l'aide de la clé de réseau

K_N. Il est donc prêt à diffuser des données sur le réseau. On notera que le dispositif source ne connaît pas la clé secrète de réseau K_N.

Les étapes ultérieures 109 à 113 illustrées à la figure 2 concernent la transmission de données « utiles », c'est à dire typiquement des données audio vidéo embrouillées.

Les données reçues par le dispositif source 1 comportent des messages ECM. Le dispositif source déchiffre ces derniers pour en extraire les mots de contrôle CW puis il chiffre les mots de contrôle CW à l'aide de la clé symétrique K_C par l'intermédiaire d'un algorithme de chiffrement symétrique E3 (étape 109). Le dispositif source 1 réinsère ensuite ces mots de contrôle chiffrés (i.e. $E3\{K_C\}(CW)$) dans le flux de données et transmet l'ensemble sur le bus 4 à destination du ou des dispositifs de présentation présents sur le réseau (étape 110). Le dispositif source envoie également lors de l'étape 110 la clé K_C chiffrée à l'aide de K_N qu'il avait précédemment mémorisée à l'étape 108. En pratique, les données $E2\{K_N\}(K_C)$ et $E3\{K_C\}(CW)$ sont insérées dans le message LECM qui est transmis avec les données « utiles » embrouillées E4{CW}(<Données>).

On notera également que les données utiles transmises à l'étape 110 sont chiffrées selon un algorithme de chiffrement symétrique E4 à l'aide des mots de contrôle CW.

Le dispositif de présentation 2 qui reçoit les données transmises à l'étape 110 déchiffre tout d'abord $E2\{K_N\}(K_C)$ à l'aide de K_N pour obtenir la clé K_C qui est mémorisée (étape 111) et, à l'aide de K_C, il peut déchiffrer $E3\{K_C\}(CW)$ pour accéder aux mots de contrôle CW (étape 112) et ainsi désembrouiller les données utiles (étape 113).

Les algorithmes de chiffrement symétriques E2, E3 et E4 peuvent être identiques ou différents. On pourra utiliser par exemple l'algorithme « AES » (pour « Advanced Encryption Standard » – aussi appelé « Rijndael » – et décrit par J. Daemen et V. Rijmen dans « *Proceedings from the First Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology (NIST), août 1998* »), ou encore l'algorithme « TwoFish » (décrit dans l'article « *TwoFish – a Block Encryption Algorithm* » de B. Schneier, J. Kelsey, D. Whiting, D. Wagner, N. Ferguson et publié dans le même rapport de conférence NIST).

III] Renouvellement de la clé symétrique K_C

Lorsqu'il est nécessaire de renouveler la clé K_C, notamment avant de diffuser un nouveau contenu numérique sur le réseau, on pourrait envisager d'utiliser le même protocole que celui décrit à la figure 2 (étapes 101 à 108). Néanmoins, ce protocole implique des calculs de chiffrement utilisant des algorithmes asymétriques qui exigent une puissance de calcul assez importante et qui sont relativement long à mettre en œuvre dans des processeurs de carte à puce. C'est pourquoi, pour le renouvellement de la symétrique « court terme » K_C, un second protocole est utilisé.

Ce second protocole permettant le renouvellement de la clé symétrique K_C est illustré par la figure 5.

Selon ce protocole, lors d'une première étape 400, le dispositif source 1 (ou plus précisément son module convertisseur 12) génère un nombre aléatoire D et il le mémorise. Il calcule ensuite (étape 401) la nouvelle clé symétrique K'_C en appliquant une fonction f à la clé K_C mémorisée lors du premier protocole (à l'étape 103) et au nombre D. La fonction f est notamment une fonction de dérivation classique telle qu'une fonction de hachage (on peut par exemple utiliser la fonction SHA-1 décrite dans le document « *Secure Hash Standard, FIPS PUB 180-1, National Institute of Standard Technology, 1995* ») ou bien encore une fonction de cryptage telle que la fonction XOR. C'est une fonction dite « à sens unique » (« one way function » en anglais), c'est-à dire que, connaissant le résultat $f(K_C, D)$ et le nombre D, il est impossible de retrouver la clé K_C.

L'étape 402 correspond à l'étape 109 du protocole de la figure 2 et consiste à extraire les messages ECM inclus dans les données reçues par le dispositif source pour les déchiffrer dans le module CA 14 et en extraire les mots de contrôle CW qui sont ensuite chiffrés dans le module convertisseur en utilisant la nouvelle clé symétrique K'_C. Par contre la diffusion des données « utiles » sur le réseau par le dispositif source est un peu différente de celle effectuée à l'étape 110.

En effet, à l'étape 403, le dispositif source insère dans le message LECM la donnée D générée à l'étape 400. Il insère en outre dans ce message LECM :

- la clé symétrique K_C initiale chiffrée avec la clé du réseau K_N ($E2\{K_N\}(K_C)$) et

- un ou des mots de contrôle CW chiffré(s) avec la nouvelle clé symétrique K'_C ($E3\{K'_C\}(CW)$).

Lorsque le dispositif de présentation 2 reçoit les données diffusées à l'étape 403, il déchiffre tout d'abord $E2\{K_N\}(K_C)$ avec la clé du réseau K_N (étape 404), puis il calcule la nouvelle clé symétrique K'_C à partir de K_C et de D en appliquant la fonction f (étape 405). Ayant obtenu K'_C, il peut ensuite déchiffrer $E3\{K'_C\}(CW)$ pour obtenir le mot de contrôle CW (étape 406) et désembrouiller les données « utiles » à l'aide de ce mot de contrôle (étape 407).

Grâce à ce protocole, il n'est pas nécessaire d'effectuer un échange de données entre un dispositif source et un dispositif récepteur pour obtenir le renouvellement d'une clé symétrique K'_C. Ceci est particulièrement avantageux par exemple lorsque aucun dispositif de présentation n'est en état « d'éveil » dans le réseau et qu'un utilisateur souhaite enregistrer un programme (contenu numérique) reçu par le dispositif source. Le dispositif source pourra ainsi renouveler sa clé de chiffrement symétrique K_C sans avoir besoin d'un quelconque dispositif de présentation et pourra donc diffuser des données utiles accompagnées de messages LECM protégés par cette clé renouvelée pour que les données soient enregistrées dans une unité de stockage numérique telle que le magnétoscope 3 de la figure 1.

REVENDICATIONS

1. Procédé de renouvellement de clé symétrique dans un réseau de communication comprenant un dispositif d'un premier type (1) contenant :

- une première clé symétrique (K_C) pour chiffrer des données (CW) à transmettre à un dispositif d'un second type raccordé au réseau ; et
- ladite première clé symétrique (K_C) chiffrée ($E2\{K_N\}(K_C)$) avec une seconde clé symétrique de réseau (K_N) connue seulement d'au moins un dispositif d'un second type (2) raccordé audit réseau ;

le procédé comportant les étapes qui consistent, pour le dispositif d'un premier type, à :

(a) générer un nombre aléatoire (D) ;

(b) calculer une nouvelle clé symétrique (K'_C) fonction de la première clé symétrique (K_C) et dudit nombre aléatoire (D) ;

(c) chiffrer les données à transmettre (CW) avec la nouvelle clé symétrique (K'_C) ; et

(d) transmettre à un dispositif d'un second type (2), via ledit réseau :

- les données chiffrées avec la nouvelle clé symétrique ($E3\{K'_C\}(CW)$) ;
- le nombre aléatoire (D) ; et
- ladite première clé symétrique chiffrée avec la seconde clé symétrique de réseau ($E2\{K_N\}(K_C)$).

2. Procédé selon la revendication 1, dans lequel la fonction (f) utilisée pour le calcul de la nouvelle clé symétrique (K'_C) est une fonction de dérivation à sens unique.

3. Procédé selon la revendication 2, dans lequel la fonction (f) est une fonction de hachage ou de cryptage.

4. Procédé selon l'une des revendications précédentes, comportant en outre les étapes consistant, pour le dispositif d'un second type (2) qui reçoit les données transmises à l'étape (d), à :

(e) déchiffrer, avec la seconde clé symétrique de réseau (K_N), le chiffrement ($E2\{K_N\}(K_C)$) de la première clé symétrique (K_C) ;

(f) déterminer, en fonction de la première clé symétrique (K_C) obtenue à l'étape (e) et dudit nombre aléatoire (D), la nouvelle clé symétrique (K'_C) ; et

(g) déchiffrer les données reçues avec la nouvelle clé symétrique (K'_C) ainsi obtenue.

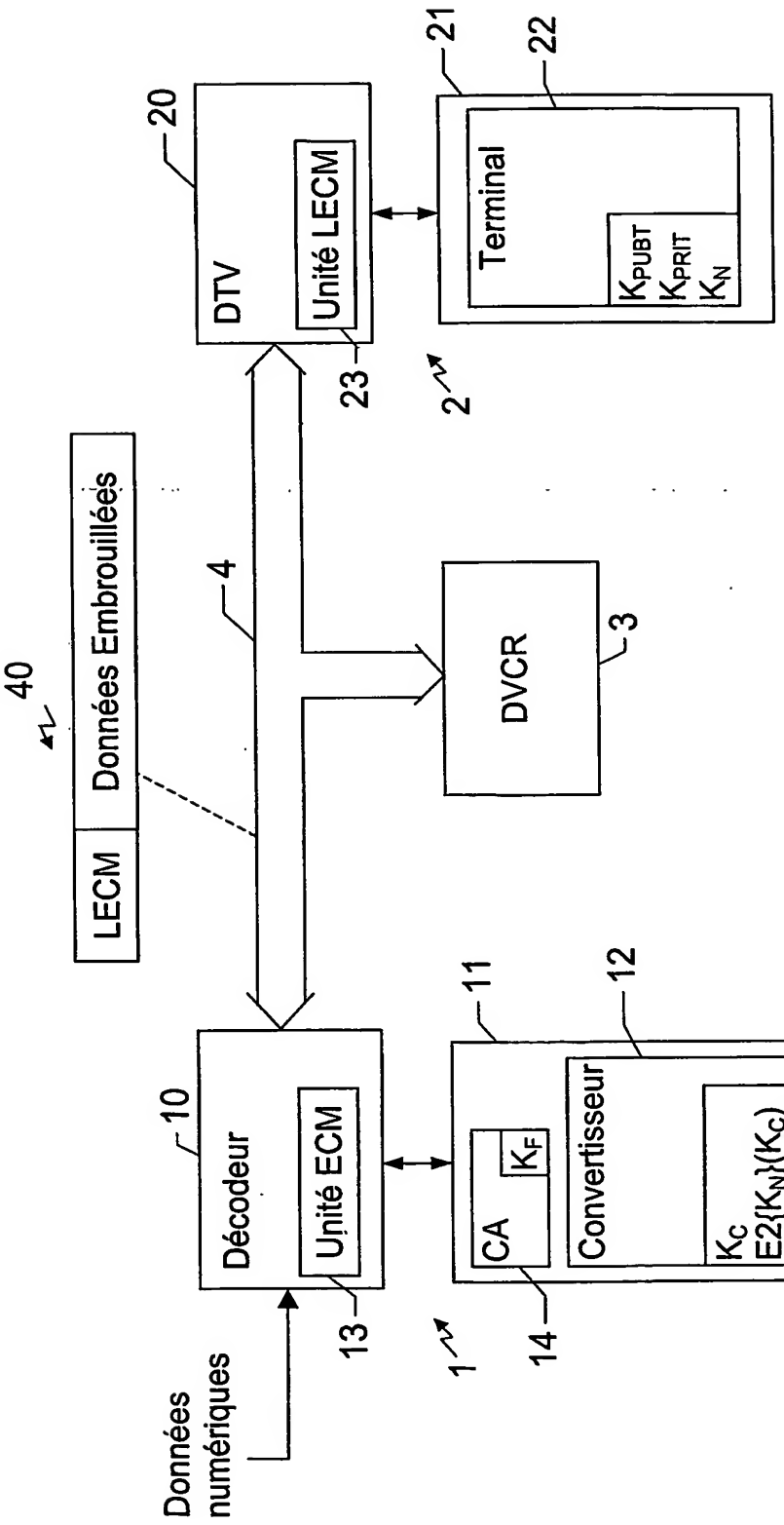

20
DTV
Unité LECM
23
21
22
Terminal
K_{PUBT}
K_{PRIT}
K_N
2
40
LECM
Données Embrouillées
4
DVCR
3
10
Décodeur
Unité ECM
13
11
12
CA
K_F
Convertisseur
K_C
$E2(K_N)(K_C)$
14
1
Données numériques

Fig. 1

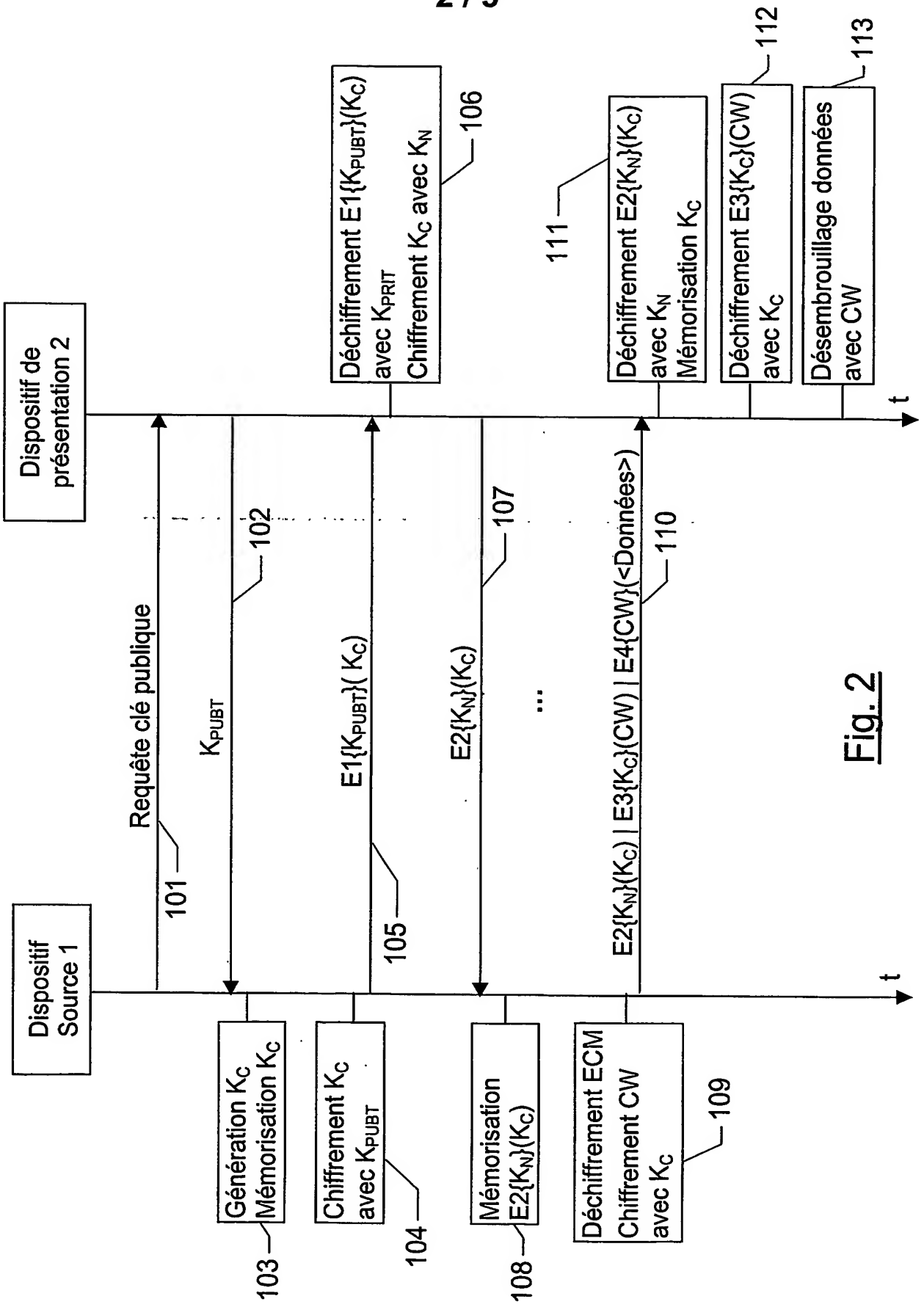

Dispositif Source 1
Dispositif de présentation 2
Requête clé publique
101
K_{PUBT}
102
Génération K_C Mémorisation K_C
103
Chiffrement K_C avec K_{PUBT}
104
$E1\{K_{PUBT}\}(K_C)$
105
Déchiffrement $E1\{K_{PUBT}\}(K_C)$ avec K_{PRIT} Chiffrement K_C avec K_N
106
$E2\{K_N\}(K_C)$
107
Mémorisation $E2\{K_N\}(K_C)$
108
Déchiffrement ECM Chiffrement CW avec K_C
109
$E2\{K_N\}(K_C) \mid E3\{K_C\}(CW) \mid E4\{CW\}(<Données>)$
110
Déchiffrement $E2\{K_N\}(K_C)$ avec K_N Mémorisation K_C
111
Déchiffrement $E3\{K_C\}(CW)$ avec K_C
112
Désembrouillage données avec CW
113
t
t

Fig. 2

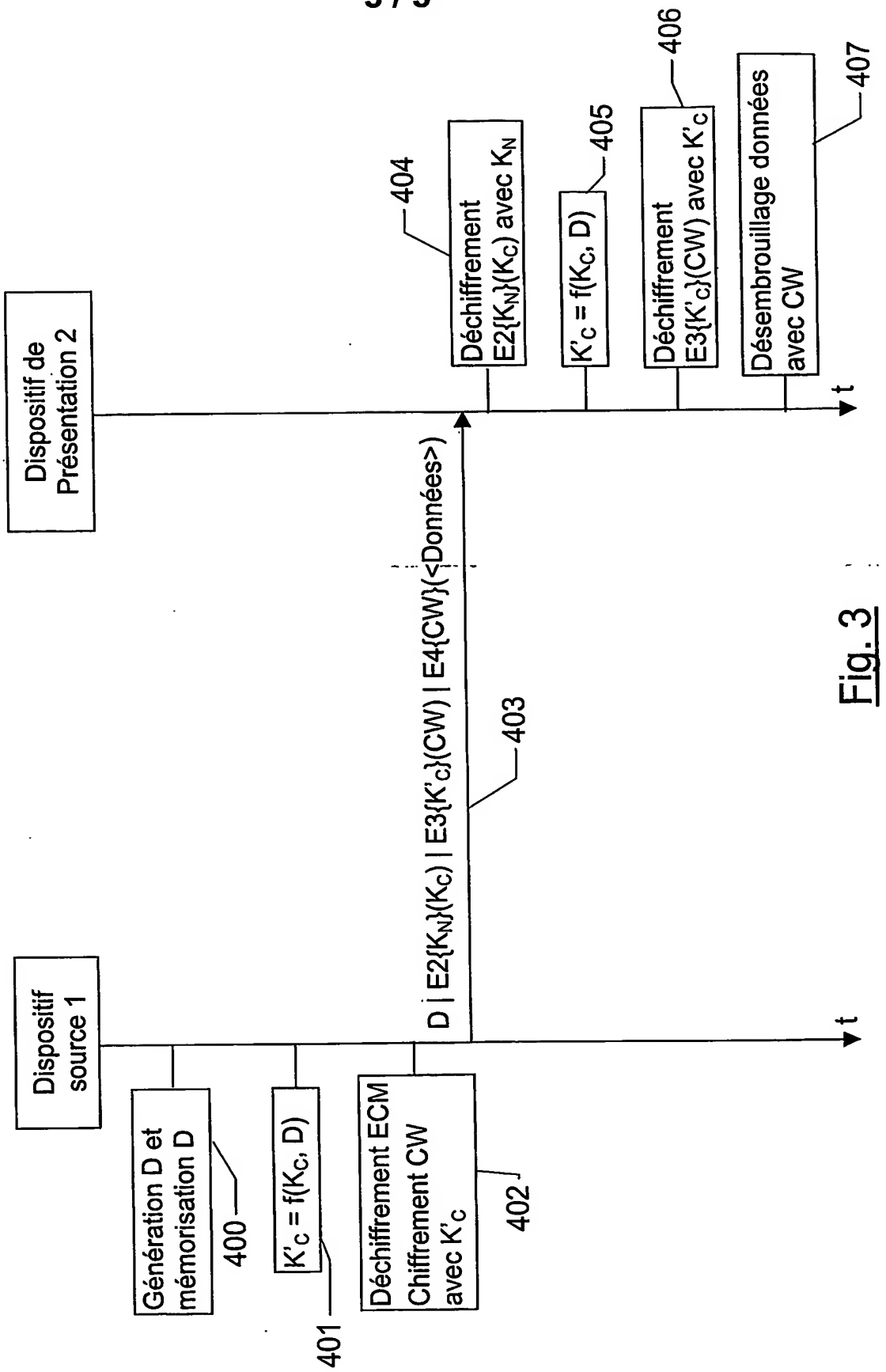

Dispositif source 1
Dispositif de Présentation 2
Génération D et mémorisation D
400
K'c = f(Kc, D)
401
Déchiffrement ECM Chiffrement CW avec K'c
402
D | E2{KN}(Kc) | E3{K'c}(CW) | E4{CW}(<Données>)
403
Déchiffrement E2{KN}(Kc) avec KN
404
K'c = f(Kc, D)
405
Déchiffrement E3{K'c}(CW) avec K'c
406
Désembrouillage données avec CW
407
t
t

Fig. 3

INTERNATIONAL SEARCH REPORT

Int ational Application No
PCT/FR 03/03250

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENEZES ET AL: "Handbook of Applied Cryptography, PASSAGE" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 497-552, XP002248262 ISBN: 0-8493-8523-7 page 497-499 page 551-552 ---	1-4
A	CA 2 381 110 A (THOMSON LICENSING SA) 25 October 2002 (2002-10-25) page 8, line 11 -page 9, line 6; claims 1,2 page 13, line 1 -page 14, line 35 figure 4 ---	1-4
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 March 2004	14/04/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Olaechea, F

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/03250

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YU-LUN HUANG ET AL: "Practical key distribution schemes for channel protection" COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE, 2000. COMPSAC 2000. THE 24TH ANNUAL INTERNATIONAL TAIPEI, TAIWAN 25-27 OCT. 2000, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 25 October 2000 (2000-10-25), pages 569-574, XP010523833 ISBN: 0-7695-0792-1 the whole document	1-4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 03/03250

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CA 2381110 A	25-10-2002	FR 2824212 A1	31-10-2002
		BR 0201403 A	12-11-2002
		CA 2381110 A1	25-10-2002
		CN 1383296 A	04-12-2002
		EP 1253762 A1	30-10-2002
		HU 0201358 A2	28-01-2003
		JP 2003008566 A	10-01-2003
		PL 353583 A1	04-11-2002
		US 2003108206 A1	12-06-2003
		ZA 200203084 A	25-11-2002

RAPPORT DE RECHERCHE INTERNATIONALE

De[illegible]le internationale No
PCT/FR 03/03250

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	MENEZES ET AL: "Handbook of Applied Cryptography, PASSAGE" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 497-552, XP002248262 ISBN: 0-8493-8523-7 page 497-499 page 551-552 ---	1-4
A	CA 2 381 110 A (THOMSON LICENSING SA) 25 octobre 2002 (2002-10-25) page 8, ligne 11 -page 9, ligne 6; revendications 1,2 page 13, ligne 1 -page 14, ligne 35 figure 4 --- -/--	1-4

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
26 mars 2004	14/04/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Olaechea, F

Formulaire PCT/ISA/210 (deuxième feuille) (Janvier 2004)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/03250

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	YU-LUN HUANG ET AL: "Practical key distribution schemes for channel protection" COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE, 2000. COMPSAC 2000. THE 24TH ANNUAL INTERNATIONAL TAIPEI, TAIWAN 25-27 OCT. 2000, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 25 octobre 2000 (2000-10-25), pages 569-574, XP010523833 ISBN: 0-7695-0792-1 le document en entier	1-4

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 03/03250

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
CA 2381110 A	25-10-2002	FR 2824212 A1	31-10-2002
		BR 0201403 A	12-11-2002
		CA 2381110 A1	25-10-2002
		CN 1383296 A	04-12-2002
		EP 1253762 A1	30-10-2002
		HU 0201358 A2	28-01-2003
		JP 2003008566 A	10-01-2003
		PL 353583 A1	04-11-2002
		US 2003108206 A1	12-06-2003
		ZA 200203084 A	25-11-2002